REMARKS

In the Office Action, the Examiner rejected claims 1, 4, 8, 11, 16, 18, 20-22 under 35 U.S.C. § 102(b) as being anticipated by WEISS (U.S. Patent No. 4,998,279); rejected claims 12, 13 and 14 under 35 U.S.C. § 102(b) as anticipated by BASSENYEMUKASA et al. (U.S. Patent No. 5,623,539); rejected claim 2 under 35 U.S.C. § 103(a) as being unpatentable over WEISS in view of "Speaker Recognition in Telecom Applications" by Boves et al. ("BOVES et al."); rejected claim 3 under 35 U.S.C. § 103(a) as being unpatentable over WEISS in view SCOTT et al. (U.S. Patent No. 6,484,260); rejected claims 5 and 17 under 35 U.S.C. § 103(a) as being unpatentable over WEISS in view GELLER (U.S. Patent No. 6,199,067); rejected claim 15 under 35 U.S.C. § 103(a) as being unpatentable over BASSENYEMUKASA et al. in view of GELLER; rejected claims 6 and 7 under 35 U.S.C. § 103(a) as being unpatentable over WEISS in view of PARE, Jr. et al. (U.S. Patent No. 5,802,199); and rejected claims 9, 10 and 19 under 35 U.S.C. § 103(a) as being unpatentable over WEISS in view of the AKHTERUZZAMAN et al. (U.S. Patent No. 5,406,619)

Claims 1-22 are pending in the present application. Reconsideration and allowance of all claims in view of the following remarks is respectfully requested.

Claims 1, 4, 8, 11, 16, 18, 20-22 have been rejected under 35 U.S.C. § 102(b) as being anticipated by WEISS. Applicant respectfully traverses.

Independent claim 1, for example, recites a method of validating a user for a transaction to be effectuated by using a transaction card. The method includes: configuring a biometric profile for the user, where the biometric profile includes a plurality of biometric samples related to the user; associating the biometric profile with

an indicium assigned to the transaction card; biometrically interrogating the user when the transaction is attempted by the user; monitoring a biometric response generated with respect to the user in response to the step of biometric interrogation; determining if the biometric response matches a biometric sample in the biometric profile; and if so approving the user for the transaction.

A proper rejection under 35 U.S.C. § 102 requires that a reference teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. See M.P.E.P. § 2131. WEISS does not disclose or suggest the combination of features recited in Applicant's claim 1.

For example, WEISS does not disclose or suggest associating the biometric profile with an indicium assigned to the transaction card, as required by claim 1. The Examiner relied upon col. 3, line 22-24 of WEISS as allegedly disclosing the claimed feature (Office Action, pg. 2). Applicant respectfully submits that this section of WEISS does not disclose or suggest either a transaction card or the step of associating an indicium to the transaction card, as currently recited.

At col. 3, line 22-24, WEISS discloses:

> In practice, the user will initially input his PIN or other identifying code on telephone 518A. While this may be done orally, it is preferably done by striking appropriate keys on the telephone to provide a digital indication.

This section of WEISS discloses entering a PIN or other identifying code associated with the user into the user's telephone when identity verification is desired. The PIN is received by a verification device and results in the generation of a time varying multi-character code that matches a time varying multi-character card generated at a user device (WEISS, Abstract). This section of WEISS does not disclose or suggest

associating the biometric profile with an indicium associated with a transaction card. Rather, the PIN received in WEISS is associated with the user. Additionally, this section of WEISS does not disclose that a transaction is being effectuated by using a transaction card. For at least the foregoing reasons WEISS does not anticipate claim 1.

Claim 4 depends from claim 1. Therefore, Applicant submits that claim 4 is not anticipated by WEISS for at least the reasons given above with respect to claim 1. Moreover, claim 4 recites features not disclosed or suggested by WEISS.

For example, claim 4 recites prompting the user to input the indicium assigned to the transaction card if the biometric response does not match a biometric sample of the biometric profile. The Examiner relied on col. 3, lines 22, 24-25 of WEISS for allegedly disclosing this feature (Office Action, pg. 3). Applicant submits that this section of WEISS does not disclose this feature of claim 4.

At col. 3, lines 22, 24-25, WEISS discloses:

> In practice, the user will initially input his PIN or other identifying code on telephone 518A. While this may be done orally, it is preferably done by striking appropriate keys on the telephone to provide a digital indication.

This section of WEISS discloses *initially* entering a PIN or other identifying code associated with the user into the user's telephone when identity verification is desired and *prior to* voice authentication being performed. The PIN is received by a verification device and results in the generation of a time varying multi-character code that matches a time varying multi-character card generated at a user device (see, additionally, WEISS cols. 3-4). This section of WEISS in no way discloses or suggests prompting a user to input the indicium if the biometric response does not match a biometric sample of the biometric profile.

For at least this additional reason, Applicant submits that claim 4 is not anticipated by WEISS.

Independent claim 8 recites features similar to features recited above with respect to claim 1. Therefore, Applicant submits that claim 8 is not anticipated by WEISS for at least the reasons given above with respect to claim 1. Moreover, claim 8 recites features not disclosed or suggested by WEISS.

For example, claim 8 recites configuring a personalized profile for the user, where the personalized profile includes a plurality of voice samples elicited from the user in response to a plurality of personalized questions directed to the user. The Examiner relied on col. 3, lines 49-52 for allegedly disclosing this feature (Office Action, pg. 3). Applicant submits that this section of WEISS does not disclose this feature of claim 8.

At col. 3, lines 49-52, WEISS discloses:

> Character voice pattern store 530 stores a predetermined number of samples from the voice pattern of each individual using the system speaking each character which may appear on display 514.

This section of WEISS discloses the manner in which voice samples are received from a user for storage and subsequent use in authenticating the user. WEISS discloses that the system only stores samples of users speaking each character which may appear on the display of the user device. This section of WEISS does not disclose or suggest the feature of eliciting voice samples from the user in response to a plurality of personalized questions directed to the user.

Claim 8 also recites querying the user for a voice response to a question that is randomly selected from the the plurality of personalized questions. The Examiner relied on col. 1, lines 64-66 of WEISS for allegedly disclosing this feature (Office Action, pg.

3). Applicant submits that this section of WEISS does not disclose this feature of claim 8.

At col. 3, lines 64-66, WEISS discloses:

> The individual communicates the nonpredictable code generated at a given time to a verification device in a manner such that a biocharacteristic of the user is communicated with each code character.

This section of WEISS discloses that each character of a nonpredictable code is biometrically communicated to a verification device. The nonpredictable code is generated by a user device (see WEISS col. 1, lines 60-64). This section of WEISS does not disclose or suggests the claimed feature of querying the user for a voice response to a question that is randomly selected from the plurality of personalized questions. No questions are asked of the user and the nonpredictable code biometrically input by the user in WEISS is not selected from a plurality of personalized questions used to elicit responses during configuration.

For at least the foregoing reasons, Applicant submits that claim 8 is not anticipated by WEISS.

Claim 11 recites features similar to features recited above with respect to claim 8. Therefore, Applicant submits that claim 11 is not anticipated by WEISS for reasons similar to the reasons given above with respect to claim 8. Moreover, claim 11 recites features not disclosed or suggested by WEISS.

For example, claim 11 recites prompting the user to input the indicium assigned to the calling card after verifying that the voice response does not match a corresponding voice sample in the voice profile. The Examiner relied on col. 3, lines 22, 24-25 of

WEISS for allegedly disclosing this feature (Office Action, pg. 3). Applicant submits that this section of WEISS does not disclose this feature of claim 4.

At col. 3, lines 22, 24-25, WEISS discloses:

> In practice, the user will initially input his PIN or other identifying code on telephone 518A. While this may be done orally, it is preferably done by striking appropriate keys on the telephone to provide a digital indication.

This section of WEISS discloses *initially* entering a PIN or other identifying code associated with the user into the user's telephone when identity verification is desired and *prior to* voice authentication being performed. The PIN is received by a verification device and results in the generation of a time varying multi-character code that matches a time varying multi-character card generated at a user device (see, additionally, WEISS cols. 3-4). This section of WEISS in no way discloses or suggests prompting a user to input the indicium if the voice response does not match a corresponding voice sample in the voice profile.

For at least this additional reason, Applicant submits that claim 11 is not anticipated by WEISS.

Independent claim 16 recites features similar to features recited above with respect to claim 1. Therefore, Applicant submits that claim 16 is not anticipated by WEISS reasons similar to the reasons given above with respect to claim 1.

Claims 18 and 20-22 depend from claim 16. Therefore these claims are not anticipated by WEISS for at least the reasons given above with respect to claim 16.

Claims 12-14 have been rejected under 35 U.S.C. § 102(b) as being anticipated by BASSENYEMUKASA et al. Applicant respectfully traverses.

Independent claim 12, for example, recites a fraud prevention method for use in a transaction-card-based system having a conventional authentication process. The method includes determining, by utilizing the conventional authentication process, if a fraudulent transaction is being attempted in the transaction-card-based system by a user using a transaction card; if so, biometrically interrogating the user to obtain a biometric sample from the user; and upon obtaining the biometric sample, denying access to the user for the transaction in the transaction-card-based system if the biometric sample does not match an entry stored in a biometric profile database inherently associated with the transaction card's owner.

A proper rejection under 35 U.S.C. § 102 requires that a reference teach every aspect of the claimed invention either explicitly or impliedly. Any feature not directly taught must be inherently present. See M.P.E.P. § 2131. BASSENYEMUKASA et al. does not disclose or suggest the combination of features recited in Applicant's claim 12.

For example, BASSENYEMUKASA et al. does not disclose or suggest determining, by utilizing the conventional authentication process, if a fraudulent transaction is being attempted in the transaction-card-based system by a user using a transaction card. The Examiner relied upon col. 3, lines 7-10, of BASSENYEMUKASA et al. for allegedly disclosing determining, by utilizing the conventional authentication process, if a fraudulent transaction is being attempted in the transaction-card-based system by a user using a transaction card (Office Action pp. 4-5). Applicant respectfully submits that this section of BASSENYEMUKASA et al. does not disclose or suggest the claimed combination of features, as currently recited.

At col. 3, lines 7-10, BASSENYEMUKASA et al. discloses:

> The telephone call to which the transparent fraud detection technique is applied can be one that was originated using an access code, such as a telephone calling card number. The system checks the validity of the code in a standard manner (e.g., by comparing the code to a library of known valid codes) and completes a desired call only if the access code is valid.

This section of BASSENYEMUKASA et al. discloses that a standard access code may be used to complete a desired call upon entry by a caller. It does not disclose or suggest the claimed feature of determining, by utilizing a conventional authentication process, if a fraudulent transaction is being attempted. Rather, the system of BASSENYEMUKASA et al. appears to disclose that a call is connected only after a valid conventional access code has been received by the system. This conventional access system makes no determination as to the fraudulent nature of the present transaction. This section of BASSENYEMUKASA et al. does not disclose or suggest utilizing a conventional authentication process to determine whether a fraudulent transaction is being attempted, as currently recited in Applicant's claim 12.

Additionally, BASSENYEMUKASA et al. does not disclose the claimed features of biometrically interrogating the user to obtain a biometric sample from the user; and upon obtaining the biometric sample, denying access to the user for the transaction in the transaction-card-based system if the biometric sample does not match an entry stored in a biometric profile database inherently associated with the transaction card's owner. The Examiner relied upon col. 3, lines 21-23 of BASSENYEMUKASA et al. for allegedly disclosing these features (Office Action, pp. 4-5). Applicant respectfully submits that this section of BASSENYEMUKASA et al. does not disclose or suggest the claimed combination of features, as currently recited.

At col. 3, line 21-23, BASSENYEMUKASA et al. discloses:

> ... comparing each live voice pattern to each of a plurality of stored authorized user voice patterns; and determining whether the telephone line is being used by an authorized user based on the results of the comparing step.

This section of BASSENYEMUKASA et al. discloses comparing received voice patterns with a plurality of stored authorized user voice patterns and determining whether the telephone line is being used by an authorized user based on the results of this comparison. This section of BASSENYEMUKASA et al. does not disclose or suggest biometrically interrogating the user to obtain a biometric sample if the conventional authentication process has determined that a fraudulent transaction is being attempted and rejecting or denying access to the user if the biometric sample does not match an entry stored in a biometric profile database inherently associated with the transaction card's owner. Rather, BASSENYEMUKASA et al. discloses completing the call upon entry of a valid conventional access code (see previously cited section, col. 3, lines 7-10). The transparent fraud detection technique of BASSENYEMUKASA et al. is only implemented once the call is connected.

For at least the foregoing reasons, Applicant submits that claim 12 is not anticipated by BASSENYEMUKASA et al.

Claims 13-14 depend from claim 12. Therefore, these claims are not anticipated by BASSENYEMUKASA et al. for at least the reasons given above with respect to claim 12.

Claim 2 was rejected under 35 U.S.C. § 103(a) as being unpatentable over WEISS in view of BOVES et al. Applicant respectfully traverses.

Claim 2 depends on claim 1. Applicant submits that the disclosure of BOVES et al. does not remedy the deficiencies in the disclosure of WEISS as set forth above with

respect to claim 1. Therefore, Applicant submits that claim 2 is patentable over WEISS and BOVES et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1. Additionally, claim 2 recites features not disclosed or suggested by WEISS and BOVES et al.

For example, claim 2 recites the method of validating a user for a transaction as set forth in claim 1, wherein a portion of the plurality of biometric samples comprises voice samples generated by the user responsive to a plurality of questions directed to the user in the configuration step, and further wherein the step of biometric interrogation involves querying the user for voice response to a randomly selected question of the plurality of questions. WEISS and BOVES et al., whether taken alone or in any reasonable combination, do not disclose or suggest this claimed combination of features.

For example, WEISS and BOVES et al. do not disclose or reasonably suggest that a portion of the plurality of biometric samples comprise voice samples generated by the user in response to a plurality of questions directed to the user during configuration. The Examiner admitted that WEISS does not disclose this feature and does not appear to rely on any alleged teaching of BOVES et al. to remedy this noted deficiency (Office Action, pp. 5-6). Moreover, it is clear that BOVES et al. does not to disclose or suggest voice samples being generated by the user in response to a plurality of questions directed to the user during configuration. In fact, BOVES et al. does not speak to the manner in which voice samples are enrolled into the recognition system.

The cited WEISS and BOVES et al. references also do not disclose or suggest that the biometric interrogation involves querying the user for a voice response to a randomly selected question of the plurality of questions. The Examiner admitted that WEISS does

not disclose this feature and relied on pg. 203, col. 2 of BOVES et al. (paragraph beginning "Text-prompted") for allegedly disclosing a speaker verification system (SV) that will select a random utterance, read it to the caller, and ask the caller to repeat it (Office Action, pg. 6). More particularly, the Examiner indicates that the disclosed SV system will ask the claimant to repeat random digit sequences, or a random sequence of numbers between 21 and 99 (Office Action, pp. 5-6). Applicant respectfully submits that this section of BOVES et al. does not disclose or suggest the feature of querying the user for a voice response to a randomly selected question of the plurality of questions, as currently recited.

At pg. 203, col. 2 (paragraph beginning "Text-prompted"), BOVES et al. discloses:

> **Text-prompted** SV solves the problem that SV systems can be fooled by playing a recording of a speaker saying her or his password. Text-prompted SV systems will select a random utterance, read it to the caller, and ask the caller to repeat it verbatim. Simple forms of text-prompted SV will ask the claimant to repeat random digit sequences, or random sequences of numbers between 21 and 99.

This section of BOVES et al. discloses a speaker verification system which utilizes random utterances to elicit voice responses from callers. This section of BOVES et al. does not disclose or suggest the claimed feature of querying the user for a voice response to a randomly selected question of the plurality of questions. No previously received information from callers appear to be the basis for the SV system disclosed in BOVES et al. Rather, completely random utterances are used to elicit responses.

For at least the foregoing reasons, Applicant respectfully submits that claim 2 is patentable over WEISS and BOVES et al., whether taken alone or in any reasonable combination.

Claim 3 was rejected under 35 U.S.C. § 103(a) as being unpatentable over WEISS in view of SCOTT et al. Applicant respectfully traverses.

Claim 3 depends on claim 1. Applicant submits that the disclosure of SCOTT et al. does not remedy the deficiencies in the disclosure of WEISS as set forth above with respect to claim 1. Therefore, Applicant submits that claim 3 is patentable over WEISS and SCOTT et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1. Moreover, claim 3 recites additional features not disclosed or suggested by WEISS and SCOTT et al.

For example, claim 3 recites the method of validating a user for a transaction as set forth in claim 1, further comprising prompting the user to input the indicium assigned to the transaction card after determining that the biometric response matches a biometric sample of the biometric profile; determining if the indicium is a valid personal identification number operating as a password associated with the transaction card; and denying access to the user for the transaction if the indicium is not a valid identification number associated with the transaction card. WEISS and SCOTT et al., whether taken alone or in any proper combination, do not disclose or suggest this combination of features.

For example, WEISS and SCOTT et al. do not disclose or suggest the feature of prompting the user to input the indicium assigned to the transaction card after determining that the biometric response matches a biometric sample of the biometric profile. The Examiner admitted that that WEISS does not disclose this feature and relied on col. 2, lines 15-20 and Fig. 8 of SCOTT et al. to remedy this noted deficiency (Office Action, pp. 6-7). Applicant respectfully submits that these sections of SCOTT et al. do

not disclose or suggest the feature of prompting the user to input the indicium after determining that the biometric response matches a biometric sample of the biometric profile, as currently recited.

At col. 2, lines 15-20 SCOTT et al. discloses:

> The processing unit can include a processor circuit, a memory and an encoder, wherein the memory stores the biometric data, and wherein the verification signal includes an encrypted signal encrypted by the encoder. In one embodiment, the encoder includes an encoding circuit, and the verification signal further includes an ID code indicative of the enrolled person or the device.

This section of SCOTT et al. discloses that a processing unit generates a verification signal that may include an ID code indicative of the user. This section does not disclose a user validation system which prompts a user for an indicium associated with a transaction card where it is determined that a biometric response matches a biometric sample in a biometric profile. In fact, the SCOTT et al. system does not prompt the user for any action regarding his ID code if a biometric match is made. Rather, the verification signal and its embedded ID code are automatically generated by the portable personal identification device upon biometric validation of the user.

The Scott et al. reference relates to a portable personal ID device which receives user biometric information. If the received information matches stored information, a verification signal is generated by the portable personal ID device and transmitted to a remote host system, enabling access to the host system (See SCOTT et al., Summary of the Invention). Essentially, the goal of the system of SCOTT et al. is to reduce storage overhead and processing requirements by offloading these previously centralized processes from the host system to a personal user device. SCOTT et al. does not disclose or reasonable suggest the feature of prompting the user to input indicium after

determining that the biometric response matches a biometric sample of the biometric profile, as currently recited.

For at least the foregoing reasons, Applicant respectfully submits that claim 3 is patentable over WEISS and SCOTT et al., whether taken alone or in any reasonable combination.

Claims 5 and 17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over WEISS in view the GELLER. Applicant respectfully traverses.

Claim 5 depends on claim 1. Applicant submits that the disclosure of GELLER does not remedy the deficiencies in the disclosure of WEISS as set forth above with respect to claim 1. Therefore, Applicant submits that claim 5 is patentable over WEISS and GELLER, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 1. Moreover, claim 5 recites additional features not disclosed or suggested by WEISS and GELLER.

For example, claim 5 recites the method of validating a user for a transaction as set forth in claim 1, wherein configuring the biometric profile for the user is effectuated manually. The Examiner admitted that that WEISS does not disclose this feature and relied on col. 16, lines 49-53 of GELLER to remedy this noted deficiency (Office Action, pg. 7). Applicant respectfully submits that this section of GELLER does not disclose or suggest that configuring the biometric profile for the user is effectuated manually.

At col. 16, lines 49 GELLER discloses:

> ...the User_Profile is stored "confidentially"--i.e. encrypted and protected by a password or by other access control means such as biometrics (e.g. a fingerprint scan, voice pattern matching, etc.) such that only the user can access and update his or her User_Profile.

This section of GELLER discloses utilizing biometrics or other access control means to protect a user profile. This section of GELLER does not disclose manually effectuating the step of configuring a biometric profile, as currently recited. Applicants are unclear how GELLER's disclosed confidential storing of a User Profile teaches or remotely suggests the claimed manual configuration feature. The combination of WEISS and GELLER neither discloses nor fairly suggests manual configuration of the biometric profile.

For at least the foregoing reasons, Applicant respectfully submits that claim 5 is patentable over WEISS and GELLER, whether taken alone or in any reasonable combination.

Claim 17 depends on claim 16. Applicant submits that the disclosure of GELLER does not remedy the deficiencies in the disclosure of WEISS as set forth above with respect to claim 16. Therefore, Applicant submits that claim 17 is patentable over WEISS and GELLER, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 16.

Moreover, claim 17 recites that a profile database entry inherently coupled to the user comprises at least one of a fingerprint, retinal scan, palm print, and implant ID chip associated with the user. The Examiner admitted that WEISS does not disclose this claimed feature and relied on col. 16, lines 49-53 of GELLER to remedy this noted deficiency (Office Action, pg. 7). As recited above, this section of GELLER discloses utilizing biometrics (e.g., fingerprint scans, etc.) or other access control means to protect a user profile. The user profile of GELLER is further utilized in performing adaptive internet searches (GELLER, Abstract). The Examiner alleged, however, that it would

have been obvious to one of ordinary skill at the time of the invention to modify WEISS as per the teachings of GELLER to such that the User Profile is stored "confidentially" (Office Action, pg. 8). The Examiner's allegation is merely conclusory. The Examiner does not logically explain why one skilled in the art would have been motivated to incorporate the biometric access control elements of GELLER into the character voice pattern store of WEISS (see WEISS, col. 3, lines 49-53). Since the Examiner has not provided any objective motivation as to why one skilled in the art would have incorporated the features of claim 17 into the WEISS system, a *prima facie* case of obviousness has not been established with respect to claim 17.

For at least the foregoing reasons, Applicants submit that claim 17 is patentable over WEISS and GELLER, whether taken alone or in any reasonable combination.

Claim 15 is rejected under 35 U.S.C. § 103(a) as being unpatentable over BASSENYEMUKASA et al. in view of the GELLER reference. Applicant respectfully traverses.

Claim 15 depends on claim 12. Applicant submits that the disclosure of GELLER does not remedy the deficiencies in the disclosure of BASSENYEMUKASA et al. as set forth above with respect to claim 12. Therefore, Applicant submits that claim 15 is patentable over BASSENYEMUKASA et al. and GELLER, whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 12.

Moreover, claim 15 recites that a profile database entry inherently coupled to the user comprises at least one of a fingerprint, retinal scan, palm print, and implant ID chip associated with the owner. The Examiner admitted that BASSENYEMUKASA et al. does not disclose this claimed feature and relied on col. 16, lines 49-53 of GELLER to

remedy this noted deficiency (Office Action, pg. 7). As recited above, this section of GELLER discloses utilizing biometrics (e.g., fingerprint scans, etc.) or other access control means to protect a user profile. The user profile of GELLER is further utilized in performing adaptive internet searches (GELLER, Abstract). The Examiner alleged, however, that it would have been obvious to one of ordinary skill at the time of the invention to modify BASSENYEMUKASA et al. as per the teachings of GELLER to such that the User Profile is stored "confidentially" (Office Action, pg. 8). The Examiner's allegation is merely conclusory. The Examiner does not logically explain why one skilled in the art would have been motivated to incorporate the biometric access control elements of GELLER into the voice information memory of BASSENYEMUKASA et al. (see BASSENYEMUKASA et al., col. 2, lines 36-50). Since the Examiner has not provided any objective motivation as to why one skilled in the art would have incorporated the features of claim 15 into the WEISS system, a *prima facie* case of obviousness has not been established with respect to claim 15.

For at least the foregoing reasons, Applicants submit that claim 15 is patentable over BASSENYEMUKASA et al. and GELLER, whether taken alone or in any reasonable combination.

Claims 6 and 7 are rejected under 35 U.S.C. § 103(a) as being unpatentable over WEISS in view the PARE, Jr. et al. Applicant respectfully traverses.

Claims 6 and 7 depend on claim 1. Applicant submits that the disclosure of PARE, Jr. et al. does not remedy the deficiencies in the disclosure of WEISS as set forth above with respect to claim 1. Therefore, Applicant submits that claims 6 and 7 are patentable over WEISS and PARE, Jr. et al., whether taken alone or in any reasonable

combination, for at least the reasons given above with respect to claim 1. Moreover, claims 6 and 7 recite additional features not disclosed or suggested by WEISS and PARE, Jr. et al.

For example, claim 6 recites the method of validating a user for a transaction as set forth in claim 1, wherein configuring a biometric profile for the user is effectuated automatically. The Examiner admitted that that WEISS does not disclose this feature and relied on col. 4, line 33-38 and col. 4, lines 42-44 of PARE, Jr. et al. to remedy this noted deficiency (Office Action, pg. 9). Applicant respectfully submits that these sections of PARE, Jr. et al. do not disclose or suggest that configuring the biometric profile for the user is effectuated automatically.

At col. 4, lines 33-38 PARE, Jr. et al. discloses:

> In another embodiment of the invention the identification computer system further comprises a purge engine for deleting biometric samples and personal identification codes from the master computer and local computer database. In order to store only biometric samples from those individuals who use the system more often...

This section of PARE, Jr. et al. discloses a purge engine for routinely removing biometric samples for users who do not use the system frequently enough. This section of PARE, Jr. et al. does not disclose automatically effectuating the step of configuring a biometric profile (e.g., when it is determined that no biometric profile currently exists), as currently recited. Applicant is unclear how GELLER's disclosed purge engine teaches or remotely suggests the claimed automatic biometric profile configuration feature. The combination of WEISS and PARE, Jr. et al. neither discloses nor fairly suggest automatic configuration of the biometric profile.

For at least the foregoing reasons, Applicant respectfully submits that claim 6 is patentable over WEISS and GELLER, whether taken alone or in any reasonable combination.

Claims 9, 10 and 19 are rejected under 35 U.S.C. § 103(a) as being unpatentable over WEISS in view of the AKHTERUZZAMAN et al. Applicant respectfully traverses.

Claims 9 and 10 depend on claim 8. Applicant submits that the disclosure of AKHTERUZZAMAN et al. does not remedy the deficiencies in the disclosure of WEISS as set forth above with respect to claim 8. Therefore, Applicant submits that claims 9 and 10 are patentable over WEISS and AKHTERUZZAMAN et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 8. Moreover, claims 9 and 10 recite additional features not disclosed or suggested by WEISS and AKHTERUZZAMAN et al.

For example, claim 9 recites populating at least a portion of the personalized profile with a plurality of Dual Tone Multi Frequency (DTMF) sample responses elicited from the user in the configuration step; prompting the user to input a DTMF response in response to the question that is randomly selected from plurality of personalized questions; verifying if the response matched a corresponding sample response in the personalized profile; and denying access to the user for the call if the response does not match the corresponding sample response in the personalized profile. WEISS and AKHTERUZZAMAN et al., whether taken alone or in any proper combination, do not disclose or suggest this combination of features.

For example, WEISS and AKHTERUZZAMAN et al. do not disclose or suggest that the step of populating at least a portion of the personalized profile with a plurality of

Dual Tone Multi Frequency (DTMF) sample responses elicited from the user in the configuration step. The Examiner admitted that that WEISS does not disclose this feature and relied on col. 2, lines 65-68 and col. 3, lines 1-2, 5-7 of AKHTERUZZAMAN et al. to remedy this noted deficiency (Office Action, pp. 9-10). Applicant respectfully submits that these sections of AKHTERUZZAMAN et al. do not disclose or suggest that the step of populating at least a portion of the personalized profile with a plurality of DTMF sample responses elicited from the user in the configuration step.

At col. 2, lines 65-68 to col. 3, lines 1-7 AKHTERUZZAMAN et al. discloses:

> The user has the option, the only option available in some presently available authentication devices, of manually keying in the number to the UA and dialing the response back to the system manually. In this case a voiced response from the system provides the user with a random number to enter into the UA. Once this is keyed into the UA by the user, the UA produces a corresponding output number on its display. This is entered by the user (using a telephone dual tone multi-frequency (DTMF) keyboard if provided or using voice if a speech-recognizing system is supported) to seek authentication.

This section of AKHTERUZZAMAN et al. discloses a universal authentication device which generates a voice response providing a user with a random number. The user enters the received number into the UA and the UA outputs a response number on its display. The user then, using the telephone keyboard, initiates a DTMF response to the system corresponding to the response number received from the UA. If the received DTMF number matches one similarly generated at the receiver, a call is allowed. Neither the WEISS reference nor the AKHTERUZZAMAN et al. reference discloses or suggests eliciting DTMF responses during the population of a personalized profile in response to questions answered during configuration, as currently recited. Rather, the DTMF responses in AKHTERUZZAMAN et al. are received during authentication and simultaneously generated by the universal authentication device and the remote

authentication system. Clearly, these DTMF tones are not included in a personalized profile in response to personalized questions asked during configuration.

For at least the foregoing reasons, Applicant respectfully submits that claim 9 is patentable over WEISS and AKHTERUZZAMAN et al., whether taken alone or in any reasonable combination.

Claims 19 depends on claim 16. Applicant submits that the disclosure of AKHTERUZZAMAN et al. does not remedy the deficiencies in the disclosure of WEISS as set forth above with respect to claim 16. Therefore, Applicant submits that claim 19 is patentable over WEISS and AKHTERUZZAMAN et al., whether taken alone or in any reasonable combination, for at least the reasons given above with respect to claim 16. Moreover, claim 19 recite additional features not disclosed or suggested by WEISS and AKHTERUZZAMAN et al.

For example, claim 19 recites that the controller comprises an Automated Response Unit associated with a Public Switched Telephone Network. The Examiner admitted that that WEISS does not disclose this feature and relied on col. 2, lines 65-68 and col. 3, lines 1-2, 5-7 of AKHTERUZZAMAN et al. to remedy this noted deficiency (Office Action, pg. 11). Applicant respectfully submits that these sections of AKHTERUZZAMAN et al. do not disclose or suggest a controller comprising an Automated Response Unit associated with a Public Switched Telephone Network.

As recited above, this section of AKHTERUZZAMAN et al. discloses a universal authentication device which generates a voice response providing a user with a random number. The user enters the received number into the UA and the UA outputs a response number on its display. The user then, using the telephone keyboard, initiates a DTMF

response to the system corresponding to the response number received from the UA. If the received DTMF number matches one similarly generated at the receiver, a call is allowed. Neither WEISS nor AKHTERUZZAMAN et al., discloses or suggests a controller comprising an Automated Response Unit associated with a Public Switched Telephone Network.

For at least the foregoing reasons, Applicant respectfully submits that claim 19 is patentable over WEISS and AKHTERUZZAMAN et al., whether taken alone or in any reasonable combination.

In view of the foregoing remarks, Applicant respectfully requests the Examiner's reconsideration of this application, and the timely allowance of the pending claims.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account No. 13-2491 and please credit any excess fees to such deposit account.

Respectfully submitted,

HARRITY & SNYDER, L.L.P.

By: Glen Snyder (Reg. No. 41,428)
For Robin C. Clark
Registration No. 40,956

Date: May 11, 2004

11240 Waples Mill Road
Suite 300
Fairfax, Virginia 22030
(571) 432-0800